

**UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION**

ECOFACOR, INC., Plaintiff, v. GOOGLE LLC, Defendant.	Case No. 6:20-cv-00075-ADA JURY TRIAL DEMANDED
ECOFACOR, INC., Plaintiff, v. ECOBEE, INC., Defendant.	Case No. 6:20-cv-00078-ADA JURY TRIAL DEMANDED
ECOFACOR, INC., Plaintiff, v. VIVINT, INC., Defendant.	Case No. 6:20-cv-00080-ADA JURY TRIAL DEMANDED

[PROPOSED] PROTECTIVE ORDER

WHEREAS, documents and information may be sought, produced or exhibited by and among the parties to the above captioned proceeding, which materials relate to trade secrets or other confidential research, development or commercial information;

IT IS HEREBY ORDERED THAT:

1. Confidential business information is information which has not been made public and which concerns or relates to the trade secrets, processes, operations, style of work, or apparatus, or to the production, sales, shipments, purchases, transfers, identification of customers, inventories, amount or source of any income, profits, losses, or expenditures of any person, firm, partnership, corporation, or other organization, the disclosure of which information is likely to have the effect of either (i) impairing the Court's ability to obtain such information as is necessary to perform its functions; or (ii) causing substantial harm to the competitive position of the person, firm, partnership, corporation, or other organization from which the information was obtained, unless the Court is required by law to disclose such information.

2. (a) Any information submitted, in pretrial discovery or in a pleading, motion, or response to a motion either voluntarily or pursuant to order, in this litigation, which is asserted by a supplier to contain or constitute confidential business information shall be so designated by such supplier in writing, or orally at a deposition, conference or hearing, and shall be segregated from other information being submitted. Documents shall be clearly and prominently marked on their face with the legends: "CONFIDENTIAL," "RESTRICTED – ATTORNEYS' EYES ONLY," or "RESTRICTED – CONFIDENTIAL SOURCE CODE." Except for paragraph 3, every provision of the Protective Order shall apply equally to the designations of "CONFIDENTIAL" and "RESTRICTED – ATTORNEYS' EYES ONLY." For avoidance of doubt, any paragraph (except paragraph 3) discussing or referring to "RESTRICTED – ATTORNEYS' EYES ONLY" is expressly incorporated by reference to apply to the "CONFIDENTIAL" designation. With regards to paragraph 3, paragraph 3(a) shall apply to the designation of "RESTRICTED – ATTORNEYS' EYES ONLY" and paragraph 3(b) shall apply to the paragraph of "CONFIDENTIAL" (collectively referred to herein as "Protected Material").

(b) The Court may determine that information alleged to be confidential is not confidential, or that its disclosure is necessary for the proper disposition of the proceeding, before, during, or after the close of a trial herein. If such a determination is made by the Court, opportunity shall be provided to the supplier of such information to argue its confidentiality prior to the time of such ruling.

3. (a) In the absence of written permission from the supplier or an order by the Court, any confidential documents or business information designated “RESTRICTED – ATTORNEYS’ EYES ONLY” submitted in accordance with the provisions of paragraph 2 above shall not be disclosed to any person other than:

- (i) outside counsel for parties to this litigation, including necessary secretarial and support personnel assisting such counsel;
- (ii) qualified persons taking testimony involving such documents or information and necessary stenographic and clerical personnel thereof;
- (iii) technical experts and their staff who are employed for the purposes of this litigation to the extent that the technical experts and their staff have agreed to be bound by the provisions of the Protective Order by signing a copy of Attachment A;
- (iv) independent litigation support services, including persons working for or as: court reporters; graphics or design services; jury or trial consulting services; and photocopy; document imaging; and litigation support or database services retained by counsel and reasonably necessary to assist counsel with the litigation of this Action; and
- (iv) the Court, the Court staff, and personnel of the Court.

(b) In the absence of written permission from the supplier or an order by the Court, any confidential documents or business information designated “CONFIDENTIAL” submitted in

accordance with the provisions of paragraph 2 above shall not be disclosed to any person other than:

(i) all persons identified in paragraph 3(a); and

(ii) up to three (3) in-house counsel for the opposing receiving party, to whom disclosure is reasonably necessary for the management, supervision, and oversight of the litigation, provided that each such person (1) is employed by the opposing receiving party and/or a parent corporation thereof that has been disclosed in this litigation under Federal Rule of Civil Procedure 7.1 and (2) has agreed to be bound by the provisions of the Protective Order by signing a copy of Attachment A; (3) is not involved in any other licensing negotiations or legal proceedings against any defendant; and (4) agrees not to participate in any other licensing negotiations or legal proceedings against any Defendant for five (5) years from the first date on which the person receives confidential documents or business information designated as CONFIDENTIAL. These provisions for in-house counsel shall not restrict or apply to disclosures between Defendants.

4. If the Court orders, or if the supplier and all parties to the litigation agree, that access to, or dissemination of information submitted as confidential business information shall be made to persons not included in paragraph 3 above, such matter shall only be accessible to, or disseminated to, such persons based upon the conditions pertaining to, and obligations arising from this order, and such persons shall be considered subject to it, unless the Court finds that the information is not confidential business information as defined in paragraph 1 hereof.

5. To the extent that any one Defendant in these above-captioned cases provides Protected Material under the terms of this Order to Plaintiff, Plaintiff shall not share that material with the other Defendants in this litigation, absent express written permission from the producing Defendant, excepting instances where there is a reasonable belief that such other Defendant

previously possessed or had access to such information in the ordinary course of business. This Order does not confer any right to any one Defendant to access the Protected Material of any other Defendant.

6. No Defendant is required to produce its Protected Material to any other Defendant or Defendants in these above-captioned cases, but nothing in this Order shall preclude such production. Notwithstanding the provisions of this Order, Plaintiff shall not disclose one Defendant's Protected Material to any other Defendant or Defendants through Court filings, oral argument in Court, expert reports, deposition, discovery requests, discovery responses, or any other means, without the express prior written consent of the Defendant that produced the Protected Material, excepting instances where there is a reasonable belief that such other Defendant previously possessed or had access to such information.

7. Any confidential business information submitted to the Court in connection with a motion or other proceeding within the purview of this litigation shall be filed under seal pursuant to paragraph 2 above.

8. The restrictions upon, and obligations accruing to, persons who become subject to this order shall not apply to any information submitted in accordance with paragraph 2 above to which the person asserting the confidential status thereof agrees in writing, or the Court rules, after an opportunity for hearing, was publicly known at the time it was supplied to the receiving party or has since become publicly known through no fault of the receiving party.

9. (a) Whenever a deposition taken on behalf of any party involves a disclosure of confidential business information of any party, the deposition or portions of the deposition must be designated as containing confidential business information subject to the provisions of this Order. Such designation must be made on the record whenever possible, but a party may designate

portions of depositions as containing confidential business information after transcription of the proceedings. A party will have up to twenty-one (21) days after receipt of the deposition transcript to inform the other party or parties to the action of the portions of the transcript to be designated “CONFIDENTIAL” or “RESTRICTED – ATTORNEYS’ EYES ONLY.” Any transcript that is prepared before the expiration of the 21-day period for designation shall be treated during that period as if it had been designated “RESTRICTED – ATTORNEYS’ EYES ONLY” in its entirety unless otherwise agreed. After the expiration of that period, the transcript shall be treated only as actually designated.

(b) a party will have the right to exclude from attendance at the deposition, during such time as the confidential business information is to be disclosed, any person other than the deponent and those entitled to receive confidential business information provided in paragraph 3.

(c) the originals of the deposition transcripts and all copies of the deposition must bear the legend “CONFIDENTIAL” or “RESTRICTED – ATTORNEYS’ EYES ONLY,” as appropriate, and the original or any copy ultimately presented to a court for filing must not be filed unless it can be accomplished under seal, identified as being subject to this Order, and protected from being opened except by order of this Court.

10. If while the litigation is before the Court, a party to this order who is to be a recipient of any business information designated as confidential and submitted in accordance with paragraph 2, disagrees with respect to such a designation, in full or in part, it shall notify the supplier in writing, and they will thereupon confer as to the status of the subject information proffered within the context of this order. If prior to, or at the time of such a conference, the supplier withdraws its designation of such information as being subject to this order, but nonetheless submits such information for purposes of the litigation, such supplier shall express the withdrawal, in writing,

and serve such withdrawal upon all parties and the Court. If the recipient and supplier are unable to concur upon the status of the subject information submitted as confidential business information within ten days from the date of notification of such disagreement, any party to this order may raise the issue of the designation of such a status to the Court who will rule upon the matter. The Court may *sua sponte* question the designation of the confidential status of any information and, after opportunity for hearing, may remove the confidentiality designation.

11. No less than 10 days (or any other period of time designated by the Court) prior to the initial disclosure to a proposed expert of any confidential information submitted in accordance with paragraph 2, the party proposing to use such expert shall submit in writing: (1) the general categories of confidential business information submitted in accordance with paragraph 2 that the party seeks permission to disclose to the proposed expert; (2) the full name of such proposed expert; (3) a copy of the proposed expert's current resume; (4) identification of the proposed expert's current employer(s); (5) each person or entity from whom the expert has received compensation or funding for work in his or her areas of expertise or to whom the expert has provided professional services, including in connection with a litigation, at any time during the preceding five years; and (6) any litigation(s) in which the proposed expert has offered expert testimony, including through a declaration, report, or testimony at a deposition or trial, during the preceding five years. If the supplier objects to the disclosure of such confidential business information to such proposed expert as inconsistent with the language or intent of this order or on other grounds, it shall within seven (7) days notify the recipient in writing of its objection and the grounds therefor. If the dispute is not resolved on an informal basis within ten days of receipt of such notice of objection, the supplier shall submit immediately the objection(s) to the Court for a

ruling. No Protected Material shall be provided to the proposed expert pending the ruling of the Court.

12. If confidential business information submitted in accordance with paragraph 2 is disclosed to any person other than in the manner authorized by this protective order, the party responsible for the disclosure must immediately bring all pertinent facts relating to such disclosure to the attention of the supplier and the Court and, without prejudice to other rights and remedies of the supplier, make every effort to prevent further disclosure by it or by the person who was the recipient of such information.

13. Nothing in this order shall abridge the right of any person to seek judicial review or to pursue other appropriate judicial action with respect to any ruling made by the Court concerning the issue of the status of confidential business information.

14. If a supplier, through inadvertence, produces any confidential business information without labeling or marking or otherwise designating it as such in accordance with this Order, the supplier may give written notice to the receiving party that the document or thing produced is deemed confidential business information, and that the document or thing produced should be treated as such in accordance with that designation under this Order. Such inadvertent or unintentional production shall not be deemed a waiver in whole or in part of a claim for confidential treatment. The receiving party must treat the materials as confidential, once the supplier so notifies the receiving party. If the receiving party has disclosed the materials before receiving the designation, the receiving party must notify the supplier in writing of each such disclosure. Counsel for the parties will agree on a mutually acceptable manner of labeling or marking the inadvertently produced materials as “RESTRICTED – ATTORNEYS’ EYES ONLY,” “CONFIDENTIAL,” or “RESTRICTED – CONFIDENTIAL SOURCE CODE.” Any

supplier that inadvertently or unintentionally produces any confidential business information without labeling or marking or otherwise designating it as such may request destruction of the produced materials by notifying the receiving party(s), as soon as reasonably possible after the supplier becomes aware of the inadvertent or unintentional disclosure, and providing replacement Protected Material that is properly designated. The receiving party(s) shall then destroy all copies of the inadvertently or unintentionally produced Protected Materials and any documents, information or material derived from or based thereon.

15. When a supplier gives notice to a receiving party that certain inadvertently produced material is subject to a claim of privilege or other protection, the obligations of the receiving party are those set forth in Federal Rule of Civil Procedure 26(b)(5)(B). This provision is not intended to modify whatever procedure may be established in an e-discovery order that provides for production without prior privilege review. Pursuant to Federal Rule of Evidence 502(d) and (e), insofar as the parties reach an agreement on the effect of disclosure of a communication or information covered by the attorney-client privilege or work product protection, the parties may incorporate their agreement in the stipulated protective order submitted to the court.

16. Upon final termination of this litigation, each party that is subject to this order shall within thirty (30) days assemble and return to the supplier all items containing confidential business information submitted in accordance with paragraph 2 above, including all copies of such matter which may have been made. Alternatively, the parties subject to this order may, with the written consent of the supplier, destroy all items containing confidential business information and certify to the supplier (or his counsel) that such destruction has taken place. This paragraph shall not apply to the Court, which shall retain such material pursuant to statutory requirements and for

other recordkeeping purposes, but may destroy such material (including electronic media containing such information) in its possession which it regards as surplusage. Notwithstanding, outside counsel of record may retain one copy of all pleadings, filings, and deposition transcripts as part of its internal records. Nothing in this paragraph requires any party or entity to delete or destroy data from emergency backup systems so long as those systems recycle and/or update their data on a revolving basis.

17. If any confidential business information which is supplied in accordance with paragraph 2 above is supplied by a nonparty to this litigation, such a nonparty shall be considered a “supplier” as that term is used in the context of this order.

18. Each nonparty supplier shall be provided a copy of this order by the party seeking information from said supplier.

19. **Source Code.** A supplier may designate documents, information, or things as “RESTRICTED – CONFIDENTIAL SOURCE CODE,” which shall mean litigation material of a supplier or of any non-parties that a supplier is permitted to produce in this litigation that constitutes or contains non-public Source Code.

A. “Source Code” shall mean source code, object code (*i.e.*, computer instructions and data definitions expressed in a form suitable for input to an assembler, compiler, or other translator), microcode, register transfer language (“RTL”), firmware, and hardware description language (“HDL”), as well as any and all programmer notes, annotations, and other comments of any type related thereto and accompanying the code. For avoidance of doubt, this includes source files, make files, intermediate output files, executable files, header files, resource

files, library files, module definition files, map files, object files, linker files, browse info files, and debug files.

B. Materials designated as “RESTRICTED – CONFIDENTIAL SOURCE CODE,” shall only be reviewable by SOURCE CODE QUALIFIED PERSONS. SOURCE CODE QUALIFIED PERSONS include the following: (1) outside litigation counsel as necessarily incident to this litigation; (2) personnel at document duplication, coding, imaging, or scanning service establishments retained by, but not regularly employed by, outside litigation counsel as necessarily incident to this litigation; (3) personnel at interpretation/translation service establishments retained by, but not regularly employed by, outside litigation counsel as necessarily incident to this litigation, including without limitation oral interpreters and document translators; (4) the Court, Court personnel and contract personnel who are acting in the capacity of Court employees as indicated in paragraph 3 of this Protective Order; (5) court reporters, stenographers and videographers transcribing or recording testimony at depositions, hearings or trial in this litigation; and (6) qualified consultants and/or qualified experts in this litigation (under paragraph 11 of the Protective Order in this litigation). Qualified consultants and/or qualified experts may only review RESTRICTED – CONFIDENTIAL SOURCE CODE after being expressly identified to the supplier as seeking access to RESTRICTED – CONFIDENTIAL SOURCE CODE. If the receiving party wishes an already identified qualified consultant or qualified expert to receive RESTRICTED – CONFIDENTIAL SOURCE CODE, it must re-comply with the provisions of paragraph 10 of this Protective Order in this litigation, including allowing the supplier an opportunity to object to this qualified consultant or qualified expert receiving RESTRICTED –

CONFIDENTIAL SOURCE CODE, and identifying the proposed qualified consultant or qualified expert as seeking access to RESTRICTED – CONFIDENTIAL SOURCE CODE.

C. Source Code shall be provided with the following additional protections:

(i) Nothing in this Protective Order shall obligate the parties to produce any Source Code, nor act as an admission that any particular Source Code is discoverable.

(ii) Access to Source Code will be given only to SOURCE CODE QUALIFIED PERSONS.

(iii) Access to Source Code shall be provided on no more than two “stand-alone” computer(s) (i.e., the computer(s) may not be linked to any network, including a local area network (“LAN”), an intranet, or the Internet, and may not be connected to any printer or storage device other than the internal hard disk drive of the computer). The stand-alone computer(s) shall be kept in a secure location at the offices of the supplier’s outside litigation counsel, or at such other location as the supplier and receiving party mutually agree. The standalone secure computer(s) may be password protected and shall have the Source Code stored on a hard drive contained inside the computer(s). The supplier shall produce Source Code in computer searchable format on the stand-alone computer(s). The stand-alone computer(s) shall, at the receiving party’s request, include reasonable analysis tools appropriate for the type of Source Code. The receiving party shall be responsible for providing the tools or licenses to the tools that it wishes to use to the supplier so that the supplier may install such tools on the standalone computer. To the extent that such tools record local working files or other records reflecting the work performed by the receiving party, such files and records shall not be reviewed, altered, or deleted by the supplier. Notwithstanding the foregoing, supplying and receiving parties may, at a

later date, agree to remote source code inspection as appropriate including, for example, by providing source code through a VPN or software solution.

(iv) The receiving party shall provide at least five (5) business days' notice to access the source code and make reasonable efforts to restrict its requests for access to the stand-alone secure computer to normal business hours, which for purposes of this paragraph shall be 9:00 a.m. through 5:30 p.m. local time at the reviewing location. The parties are to cooperate in good faith such that maintaining the Source Code at the offices of the supplier's outside litigation counsel shall not unreasonably hinder the receiving party's ability to efficiently conduct the prosecution or defense in this litigation. It is expected that access to the Source Code shall be provided at the site of any hearing or trial. Proper identification of all SOURCE CODE QUALIFIED PERSONS shall be provided prior to any access to the stand alone secure computer.

(v) All SOURCE CODE QUALIFIED PERSONS who will review Source Code on behalf of a receiving party shall be identified in writing to the supplier at least two (2) business days in advance of the first time that such person reviews such Source Code. Such identification shall be in addition to any disclosure required under paragraph 19(B) of this Protective Order. The supplier shall provide these individuals with information explaining how to start, log on to, and operate the stand-alone computer in order to access the produced Source Code on the stand-alone secure computer. For subsequent reviews by SOURCE CODE QUALIFIED PERSONS, the receiving party shall give at least one business day (and at least 24 hours') notice to the supplier of such review.

(vi) No person other than the supplier may alter, dismantle, disassemble or modify the stand-alone computer in any way, or attempt to circumvent any security feature of the computer.

(vii) No copies shall be made of Source Code, whether physical, electronic, or otherwise, other than volatile copies necessarily made in the normal course of accessing the Source Code on the stand-alone computer, except for: (1) print outs of reasonable portions of the Source Code in accordance with the provisions of paragraphs 19(C)(ix)-(x) of this Protective Order; and (2) such other uses to which the parties may agree or that the Court may order. The receiving party shall not use any outside electronic device to copy, record, photograph, or otherwise reproduce Source Code. “Reasonable portions of the Source Code” shall be limited to the portions that are necessary to understand a relevant feature of an accused product in this litigation. The supplier shall not unreasonably withhold approval and the parties shall meet and confer in good faith to resolve any disputes. The receiving party may take notes on a laptop or other personal electronic device, provided such device does not have a camera, and such notes are treated as RESTRICTED – CONFIDENTIAL SOURCE CODE under the Protective Order. The supplier may exercise personal supervision from outside the review room over the receiving party when the receiving party is in the Source Code review room. Such supervision, however, shall not entail review of attorney work product generated by the receiving party, *e.g.*, monitoring the screen of the stand-alone computer, monitoring any surface reflecting any notes or work product of the receiving party, or monitoring the key strokes of the receiving party. There will be no video supervision by any supplier.

1) To enable electronic note taking during Source Code reviews, the Supplier of Source Code shall also provide an additional “note-taking” computer loaded with at least Microsoft One Note and Microsoft Word software, unless otherwise agreed by the Supplier and the Receiving Party. The note-taking computer shall either be a portable laptop or be located in close proximity to the Source Code Computer to facilitate electronic note taking.

2) At the beginning of a Source Code review session, the Supplier shall, when requested by the reviewer, upload to the note-taking computer an encrypted notes file (*e.g.*, uploading an encrypted notes file from a USB memory stick provided by the reviewer to the note-taking computer).

3) The reviewer may then decrypt and open the notes file using the note-taking computer for the purpose of taking notes during the Source Code review session. During the source Code review session, the Supplier may disable any input and/or output devices on the note-taking computer (*e.g.*, disable any USB ports, Wi-Fi or Ethernet connectivity, and/or optical disc drives) except as necessary to enable to reviewer to take notes (*e.g.*, enable mouse and keyboard). Use or possession of any input/output device (*e.g.*, USB memory stick, mobile phone or tablet, camera or any camera-enabled device, CD, floppy disk, portable hard drive, laptop/computer, or any device that can access the Internet or any other network or external system, etc.) is prohibited while accessing the note-taking computer.

4) At the end of a Source Code review session, the reviewer may save any notes in the same encrypted notes file. The Supplier shall, when requested by the reviewer, download from the note-taking computer the encrypted notes file and provide an electronic copy to the reviewer (*e.g.*, downloading the encrypted notes file from the note-taking computer to a USB memory stick provided by the reviewer).

5) Notwithstanding this stipulation, no reviewer may at any time copy or include in electronic notes any portions or sections of the Source Code. Reviewers using electronic note-taking will be directed by undersigned counsel not to copy or include in electronic notes any portions or sections of the Source Code.

6) If requested by the Supplier, a copy of the encrypted notes file shall remain on the note-taking computer, so long as it remains encrypted.

7) If requested by the Supplier, a representative for the Supplier may oversee the transfer of the encrypted notes file from the secure data storage device to the note-taking computer, and vice-versa, without reviewing the substance of the electronic notes.

8) The reviewer shall not take notes electronically on the Source Code Computer itself or any other computer or electronic device (besides the note-taking computer) while conducting a review.

(viii) Nothing may be removed from the stand-alone computer, either by the receiving party or at the request of the receiving party, except for (1) print outs of reasonable portions of the Source Code in accordance with the provisions of paragraphs 19(C)(ix)-(x) of this Protective Order; and (2) such other uses to which the parties may agree or that the Court may order.

(ix) At the request of the receiving party, the supplier shall within three (3) business days provide one (1) hard copy print out of the specific lines, pages, or files of the Source Code that the receiving party believes in good faith are necessary to understand a relevant feature of an accused product. If the supplier objects in any manner to the production of the requested source code (*e.g.*, the request is too voluminous), it shall state its objection within the allotted two (2) business days pursuant to this paragraph. In the event of a dispute, the parties will meet and confer within five (5) business days of the objection being raised and if they cannot resolve it the parties will raise it with the Court.

(x) Hard copy print outs of Source Code shall be provided on Bates numbered and watermarked or colored paper clearly labeled RESTRICTED – CONFIDENTIAL

SOURCE CODE on each page and shall be maintained by the receiving party's outside litigation counsel or SOURCE CODE QUALIFIED PERSONS in a secured locked area. The receiving party may also temporarily keep the print outs at: (1) the Court for any proceedings(s) relating to the Source Code, for the dates associated with the proceeding(s); (2) the sites where any deposition(s) relating to the Source Code are taken, for the dates associated with the deposition(s); and (3) any intermediate location reasonably necessary to transport the print outs (*e.g.*, a hotel prior to a Court proceeding or deposition). For avoidance of doubt, an access-restricted location within the facilities of outside litigation counsel or a qualified expert, such as a conference room within an access restricted office or a locked drawer or cabinet, shall constitute a secured locked area. The receiving party shall exercise due care in maintaining the security of the print outs at these temporary locations. No further hard copies of such Source Code shall be made and the Source Code shall not be transferred into any electronic format or onto any electronic media except that:

1. The receiving party is permitted to make up to five (5) additional hard copies for use at a deposition. One hard copy of the source code may be marked as an exhibit for the deposition, and then maintained by counsel for the party presenting the exhibit during the deposition in a secured locked area. All other copies shall be destroyed immediately after the deposition is concluded. In the case of remote or video depositions, the parties should indicate beforehand that use of hard copy source code will be utilized at the deposition to ensure all counsel and the witness have a hard copy of the source code at the time of the deposition. Electronic copies of source code shall not be made or used for purposes of remote depositions.

2. The receiving party is permitted to make up to five (5) additional hard copies for the Court in connection with a Court filing, hearing, or trial, and of only the specific pages directly relevant to and necessary for deciding the issue for which the portions of the Source Code are being filed or offered. To the extent portions of Source Code are quoted in a Court filing, either (1) the entire document will be stamped and treated as RESTRICTED – CONFIDENTIAL SOURCE CODE; or (2) those pages containing quoted Source Code will be separately stamped and treated as RESTRICTED – CONFIDENTIAL SOURCE CODE.

3. Electronic copies of Source Code may be made to be included in documents which, pursuant to the Court's rules, procedures, and order(s), may be filed or served electronically. Only the necessary amount of electronic copies to effectuate such filing or service may be stored on any receiving party server, hard drive, thumb drive, or other electronic storage device at any given time. After any such electronic filing or service, the receiving party may maintain reasonable copies of such filings, but shall delete all other electronic copies of Source Code from all receiving party electronic storage devices.

4. The receiving party is permitted to possess up to seven (7) additional paper copies of the hard copy print-outs of Source Code provided by the supplier. The receiving party may provide these paper copies to qualified consultants or qualified experts, who may use such paper copies solely for active review of the source code. The receiving party is also permitted to make temporary copies necessarily made in the production of these paper copies provided any such copies are immediately deleted once the temporary copies are no longer required for the production of the paper copies. The paper copies shall not be copied in whole or in part under any other circumstances. A receiving party may destroy one or more of the seven (7) previously created paper copies and create one or more new paper copies provided that the total number in possession of the receiving party does not exceed seven (7). Absent further agreement, all paper copies shall be destroyed after the completion of the litigation or the supplying party's exit from the litigation, whichever occurs first. The receiving party shall keep and maintain a log of all custodians for all of the paper copies as well as the destruction of all paper copies.

5. The supplier shall, on request, make a searchable electronic copy of the Source Code available on a stand-alone computer during depositions of witnesses who would otherwise be permitted access to such Source Code. The receiving party shall make such request at the time of the notice for deposition.

(xi) Nothing in this Protective Order shall be construed to limit how a supplier may maintain material designated as "RESTRICTED – CONFIDENTIAL SOURCE CODE."

(xii) Outside litigation counsel for the receiving party with custody of "RESTRICTED – CONFIDENTIAL SOURCE CODE" shall maintain a source code log containing the following information: (1) the identity of each person granted access to the

“RESTRICTED – CONFIDENTIAL SOURCE CODE”; and (2) the first date on which such access was granted. Outside litigation counsel for the receiving party will produce, upon request, each such source code log to the supplier within twenty (20) days of the final determination of the litigation.

(xiii) Any print request that consists of more than 40 pages of a continuous block of source code shall be presumed to be excessive, and the burden shall be on the receiving party to demonstrate the need for such a printed copy. The receiving party may request printed source code of up to 800 pages total from each producing party. Each print request shall be made in writing to the producing party and shall include the complete path, file name, and line numbers of the source code to be printed. The parties acknowledge that they produced source code printouts in connection with U.S. ITC Investigation No. 337-TA-1185 (“the 1185 Investigation”), with the same page limits. A receiving party may request that printouts from the 1185 Investigation be deemed produced in the instant action (or re-produced with new Bates numbers, if the producing party prefers). Such a request will count toward the above page limitations. Any request for source code printouts exceeding the 800- and 40-page limits shall be made only if the requesting party has good cause to make such a request. The parties agree to negotiate, in good faith and in a timely fashion, any request exceeding these limits in order to avoid burdening the Court unnecessarily. The burden shall be on the receiving party to demonstrate the need for exceeding these limits.

20. **No prejudice.** Paragraph 19 above is without prejudice to any party’s rights to propose, request, or otherwise move for different provisions relating to source code production in this litigation.

21. **Prosecution Bar.** Any person (i) who prosecutes patents or patent applications at any time between the date on which such person subscribes to the Protective Order and the date

on which the termination of this litigation, and any appeals thereto, is final and (ii) who reviews any supplier's Confidential Business Information or RESTRICTED – CONFIDENTIAL SOURCE CODE, but excluding financial data or non-technical business information, (all of which shall also be automatically designated as 'PROSECUTION BAR MATERIALS') shall not, for a period commencing upon receipt of such information and ending two years following the absolute final termination of this litigation, prosecute patents or patent applications relating to smart thermostats or smart HVAC systems ("Prosecution Activity"). Prosecution includes, for example, original prosecution, reissue, reexamination, and any other post-grant proceedings that may affect the scope of the claims of a patent or patent application. Prosecution does not include representing a party challenging or defending a patent before an agency (including, but not limited to, a reissue protest, *ex parte* reexamination, post-grant review, or *inter partes* review), provided that there is no participation in or assistance with any claim drafting or amendment of claims in such proceedings. Nothing in this paragraph shall prevent any attorney from sending non-confidential prior art to an attorney involved in patent prosecution for purposes of ensuring that such prior art is submitted to the U.S. Patent and Trademark Office (or any similar agency of a foreign government) to assist a patent applicant in complying with its duty of candor. Nothing in this provision shall prohibit any attorney of record in this litigation from discussing any aspect of this case that is reasonably necessary for the prosecution or defense of any claim or counterclaim in this Investigation with his/her client. The parties expressly agree that the Prosecution Bar set forth herein shall be personal to any attorney who reviews PROSECUTION BAR MATERIALS and shall not be imputed to any other persons or attorneys at the attorneys' law firm. It is expressly agreed that attorneys who work on this matter without reviewing PROSECUTION BAR

MATERIALS shall not be restricted from engaging in Prosecution Activity on matters that fall within the Prosecution Bar.

22. As used herein, the term “final termination” means the availability of appeal has been exhausted, and the time for a petition of certiorari has elapsed or a petition for certiorari is denied.

23. Production of Protected Material by each of the Parties shall not be deemed a publication of the documents, information, or material (or the contents thereof) produced so as to void or make voidable whatever claim the Parties may have as to the proprietary and confidential nature of the documents, information, or other material or its contents.

24. Nothing in this Order shall be construed to effect an abrogation, waiver, or limitation of any kind on the rights of each of the Parties to assert any applicable discovery or trial privilege.

25. Documents, information or material produced in this case, including but not limited to Protected Material, shall be used by the Parties only in this case and shall not be used for any other purpose. Any person or entity who obtains access to Protected Material or the contents thereof pursuant to this Order shall not make any copies, duplicates, extracts, summaries or descriptions of such Protected Material or any portion thereof except as may be reasonably necessary in the litigation of this Action. Any such copies, duplicates, extracts, summaries or descriptions shall be classified Protected Material and subject to all of the terms and conditions of this Order. Nothing herein modifies or permits violation of a protective order in any other action, nor does it authorize the parties to use discovery from any other action to the extent it is not properly discoverable under the Federal Rules of Civil Procedure or is not otherwise consistent with the rules of any other relevant court, agency, or tribunal.

26. Each of the Parties shall also retain the right to file a motion with the Court (a) to modify this Order to allow disclosure of Protected Material to additional persons or entities if reasonably necessary to prepare and present this Action and (b) to apply for additional protection of Protected Material.

Dated: _____, 2021

Alan D. Albright
United States District Judge

Attachment A

**NONDISCLOSURE AGREEMENT FOR
REPORTER/STENOGRAPHER/TRANSLATOR**

I, _____, do solemnly swear or affirm that I will not divulge any information communicated to me in any confidential portion of the investigation or hearing in *EcoFactor, Inc. v. Google LLC*, No. 6:20-cv-00075-ADA; *EcoFactor, Inc. v. Ecobee, Inc.*, No. 6:20-cv-00078-ADA; and *EcoFactor, Inc. v. Vivint, Inc.*, No. 6:20-cv-00080-ADA, except as permitted in the protective order issued in this case. I will not directly or indirectly use, or allow the use of such information for any purpose other than that directly associated with my official duties in this case.

Further, I will not by direct action, discussion, recommendation, or suggestion to any person reveal the nature or content of any information communicated during any confidential portion of the investigation or hearing in this case.

I also affirm that I do not hold any position or official relationship with any of the participants in said investigation.

I am aware that the unauthorized use or conveyance of information as specified above is a violation of the Federal Criminal Code and punishable by a fine of up to \$10,000, imprisonment of up to ten (10) years, or both.

Signed _____

Dated _____

Firm or affiliation _____